UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,939	01/23/2004	Philip Ted Kortum	1033-T00525	5072

60533 7590 10/27/2008

TOLER LAW GROUP
8500 BLUFFSTONE COVE
SUITE A201
AUSTIN, TX 78759

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
10/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/763,939	KORTUM ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 1/23/2004; amendment filed 7/24/2008.

2. Claims 1- 26 are pending in the case.

3. No was cancelled by the applicant.

Response to Arguments

4. With regards to objection to claims 25 and 26, applicant argues that a computer-readable medium would be well understood by the one skilled in art, and therefore requires no definition in the Specification. However, the computer-readable medium as understood by the one skilled in art may include signals, which are non statutory subject material. To avoid a claim interpretation which includes said non statutory subject matter, applicants usually provide a definition of a computer-readable medium that excludes such non statutory subject matter. Applicant's Specification does not include such definition. Note that applicant's mere mention of a computer-readable medium is not sufficient to exclude such non statutory subject. Accordingly, applicant's request to withdraw the objection is respectfully denied.

With regards to objection to Specification for not explicitly defining what is meant by unique, applicant states:

"The term unique has to be taken in context. For example, claim 1 recites “A method of network authentication comprising.., generating a unique credential for the user that comprises network specific information". It would be clear to one skilled in the art that the credential would have to be unique in the network in which the authentication is taking place.”

Therefore, applicant agrees with examiner, as stated in the objection, that without a specific definition, the word unique is generally context sensitive. Applicant also fails to cite any portion of the Specification in support of how the word unique is defined. As indicated in applicant’s example cited above, applicant assumes the one skilled in art knows that the credential would have to be unique in the network in which the authentication is taking place. Additionally, claim 12 requires that the network specific information is unique to a connection in use by the user. Applicant does not discuss what is considered a **unique** network specific information associated with the connection of the user. Accordingly, the associated objection is maintained.

With regards to rejection of claims 1 and 2 under section 103, applicant argues that registration of personal information cannot be equated to common user credential. However, applicant does not cite any reason why personal information, including user phone number, and other parameters cited by Ueshima cannot be considered as user credentials. Applicant also argues that there is no teaching that the user personal information is received before the unique credential (password) is generated. However,

Ueshima col. 10, lines 27-30 clearly states that if the received telephone number belongs to any proper user, the database requests the password generating unit to generate the password. This clearly indicates that the password is generated after the credentials are received.

Applicant also argues that there is no teaching of any relationship between the receiving personal information and generating password. However, Ueshima col. 3 lines 25-58 shows that a password is generated based on user telephone number that is used by the user to connect to the authentication system (item (4)). Also see col 5 lines 1-35, or col. 8 lines 14-27. Accordingly, applicant's argument relative to allowability of claim 1 is found non persuasive.

With regards to claim 2, applicant merely states that claim 2 is dependent on claim 1, and there are additional elements not disclosed by Ueshima or Schneider, without specifically discussing any of those elements or the associated rejection. Accordingly, applicant's argument relative to allowability of claim 2 is found non persuasive.

With regards to claims 3, 4, 6, 7, 14, 15-24, applicant's argues that there is no motivation in combining conventional phones system of Ueshima with another network such as DSL, cable, ADSL, Internet, or PPPoE, as Ueshima requires that the user place a phone call to the CTI system, and it would be impossible to make a phone call if the conventional phone system is replaced by any of the networks named above. However,

first, when the conventional telephone network is replaced by any of the said networks, it would be possible to make a connection in that network, which obviously replaces the phone call as discussed by Ueshima. Second the claim requires generating a unique credential that comprises network specific information associated with a connection of the user, and wherein the connection of the user comprises a DSL, cable, ADSL, Internet, or PPPoE. When the user phone connection is replaced with any of other connections, user phone number will also be replaced with the corresponding user identifier. Accordingly, applicant's argument relative to allowability of claims 3, 4, 6, 7, 14, 15-24 is found non persuasive.

Applicant's argument relative to claims 5, 10, 13 is similar to requirements of claim 1 as discussed above. Accordingly, applicant's argument relative to allowability of claims 5, 10, 13 is found non persuasive.

With regards to claim 12, applicant argues that a phone number is not necessarily unique. However, as discussed previously, applicant fails to explicitly specify what is meant by unique. In addition, as discussed previously, in the context of authenticating a user based on the user's phone number, user's phone number is considered to be unique. Accordingly, applicant's argument relative to allowability of claim 12 is found non persuasive.

With regards to claims 25 and 26, applicant argues that the claims require replacing the credential with the network generated credential, and claim 1 and disclosure of Ueshima in view of Schneider includes the phone number as part of a certificate. Applicant emphasizes that replacing is different than including. However, the certificate may include the credential, but nevertheless, it replaces it. The certificate is not the credential. Therefore, the credential itself is not the only entity used for authentication. It is replaced by the certificate, which is not the same as the credential. Moreover, Ueshima teaches using the password for authentication, which is different than the credential (phone number) and replaces the credential. Accordingly, applicant's argument relative to allowability of claims 25 and 26 found non persuasive.

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 25 and 26 are directed to a computer-readable medium, but the term "computer-readable medium" is not defined in the Specification. It is not clear what encompasses a "computer-readable medium", and what does not.

Also, the term "unique" is used in all claims, but there is no clear and explicit definition of the word in the Specification. As a result, it is not clear what is considered unique, and what is not unique. It should be noted that an item may be considered unique in

one context, and may not be unique in another. For example, in a Wide Area Network (WAN), consisting of a plurality of Local Area Networks (LAN), the address of a device in one LAN may be unique among the address space in that LAN, but may not be unique in the WAN, because another device in another LAN may have the same address.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1 and 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima (US Patent No. 6,731,731, filed March 29, 2001) and further in view of Schneider (U.S. Patent No. 7,050,423, filed November 27, 2001).

7.1. As per claim 1, Ueshima is directed to a method of network authentication comprising (Ueshima teaches an authentication system, wherein a password is generated based on the telephone number of the device used by user, and user personal information. This generated password is sent to the user to be used for authentication): receiving a common user credential from a user seeking access to an information network (Col. 10 lines 7-30 shows that personal information of each proper

user is registered in a table of the authentication system. Col. 12 line 49 to col. 13 line 10 provides examples of user information); generating a unique credential after receiving user credential from user, the unique credential comprising network specific information associated with a connection of the user (Ueshima col. 3 lines 25-58 shows that a password is generated based on user telephone number that is used by the user to connect to the authentication system (item (4). Note that as shown in col. 10 lines 27-30, the password is generated after the credential is received). Also see col 5 lines 1-35, or col. 8 lines 14-27.); and considering the unique credential in connection with making an authentication decision for the user (the generated password is supplied to the user. The user supplies the password when calling from the same phone number, and will be authenticated based on the password and the phone number, as shown in col. 3 lines 25-58, item (6). Also see Example 3 for an operation procedure.

Ueshima teaches generating a password, supplying the password to a user, receiving the password from the user when the user wants to authenticate for a service access, and authenticating the user by verifying the submitted password. The password is generated in association with the user phone number (connection), however, Ueshima does not explicitly teach including the phone number as part of a credential.

Schneider teaches a system for supporting multiple network services, wherein requests for services are associated with the issuance of a certificate (credential) for the requesting user (see Abstract). The certificate comprises information relating to the

permitted setup, and service policy or logic representing service capabilities or service permissions, associated with the network service, and a unique setup identifier (see, for example, claim 1).

Ueshima and Schneider are analogous art as they are both directed to user authentication procedures as part of a network service system. At the time of invention, it would have been obvious to the one skilled in art to enhance Ueshima's system to use a certificate (credential), including a password, and additional fields of information, as taught by Schneider's certificate. As Ueshima bases the generation of the password on verifying the phone number used by the user, it would have been obvious to include the phone number as part of the certificate. The motivation to do so would have been to provide a more comprehensive set of authentication parameters and information relating to the permitted connection setup, by using a certificate including all said information, rather than a password alone. Note also that Ueshima's system performs authentication in two steps (see col. 9 lines 35-50), where both the phone number and the generated password are used for authentication. Therefore, an improvement to include several pieces of information in one credential containing several fields, as one suggested by Schneider, is well placed.

7.2. As per claim 2, Ueshima in view of Schneider is directed to the method of claim 1, further comprising: receiving the common user credential from a different user seeking access to the information network; generating a different unique credential for

the different user that comprises different network specific information; and considering the different unique credential in connection with making an authentication decision for the different user (As shown in Ueshima col. 10 lines 6-15, the database stores personal information for each proper user. Also, as shown in col. 3 lines 20-23, individual users are authenticated separately).

8. Claims 3-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima (US Patent No. 6,731,731, filed March 29, 2001) and further in view of Schneider (U.S. Patent No. 7,050,423, filed November 27, 2001), and further in view of Examiner Official Notice.

8.1. As per claim 3, Ueshima in view of Schneider is directed to the method of claim 1. Examiner take the Official Notice that xDSL was known as a transmission technique using telephone lines. Therefore, it would have been obvious to replace the specifics of a conventional phone line (phone number), with the specifics of xDSL links. The motivation to do so would be to expand the range of service availability, and authentication as taught by the combination of Ueshima and Scneider, and allow user access to the same services if the user uses xDSL connection instead of a conventional phone line. Therefore, Ueshima in view of Schneider and further in view of the Official Notice is directed to claim 1, wherein the connection of the user comprises an xDSL link.

8.2. As per claim 4, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, wherein the connection of the user comprises a link at least partially supported by a cable modem (See rejection of claim 3, and note that cable transmission systems were also known in the art at the time of invention).

8.3. As per claim 5, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, further comprising utilizing a network node to generate the unique credential (Ueshima col. 3 lines 38-41, indicating that the CTI server or another device generates the password).

8.4. As per claim 6, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, wherein the network specific information comprises a unique circuit identification number associated with an ADSL connection (see rejection of claim 3, and note that ADSL was known at the time of invention, and is a type of xDSL).

8.5. As per claim 7, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, wherein the network specific information comprises a virtual circuit identification associated with ADSL routing (see response to claims 3 and 6. Note that the virtual circuit identification is equivalent to a phone number).

8.6. As per claim 8, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, further comprising tracking a metric associated with the user (As shown in Schneider claim 1, information relating to the permitted setup, and service policy or logic representing service capabilities or service permissions are part of the certificate. Therefore Schneider keeps track of that information, which relates to user access control).

8.7. As per claim 9, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 8, wherein the metric is selected from the group consisting of an access control metric, a payment metric, and a security metric (see rejection of claim 8, where it is shown that an access control metric is tracked).

8.8. As per claim 10, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, further comprising utilizing a network node to generate the unique credential, wherein the network node comprises an authentication server and an interface operable to receive the common user credential (Ueshima col. 3 lines 38-41, indicating that the CTI server or another device generates the password. The CTI server authenticates the user, and therefore, it is an authentication server. Also, the authentication server receives user credentials for

purpose of authentication, therefore, it must have an interface to receive the information).

8.9. As per claim 11, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, further comprising: determining that the user does not have access rights to the information network; and initiating communication of a deny response (Ueshima col. 13 lines 40 to 45).

8.10. As per claim 12, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, wherein the network specific information comprises network generated information that is unique to a connection in use by the user (the password is generated in accordance with the phone number of the user. The phone number of the user that is used for connection is unique).

8.11. As per claim 13, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the method of claim 1, wherein the network specific information comprises information that is unique to a physical location of the user (Ueshima teaches registering the address of the user (col. 13 line 9-11). Therefore it would have been obvious to include user address in the certificate. The motivation would be to improve the security by using additional verification parameters).

8.12. As per claim 14, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to an authentication system, comprising: an interface operable to receive an authentication request (Fig. 1 and associated text, as it is the platform for performing operations described in rejection of claims 1-13), item 30 has several interfaces to receive an authentication request) from a PPPoE client of a given user (as discussed in rejection of claims 3, 4, and 7, it would have been obvious to the one skilled in art to replace networks specifics of a conventional phone system, with specifics of other types of networks, such as cable, Internet, Ethernet or Point to Point Protocol over Ethernet (PPPoE)); a customizing engine communicatively coupled to the interface and operable to add a unique identifier for the given user to the authentication request (Fig. 1 item 30. Note that it adds the password received from Password Generation unit 41, as described by combination of Ueshima in view of Schneider, and further in view of Examiner Official Notice outlined in claims 1-13); and an output device communicatively coupled to the customizing engine and operable to output the unique identifier to an access engine for authentication of the given user (item 30 has output devices for outputting the password to the Authentication System Unit).

8.13. As per claim 15, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 14, further comprising a network node that comprises the interface, the customizing engine, and the output device (item 30 is a network node, as it is connected to Network 150).

8.14. As per claim 16, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 14, further comprising the access engine, wherein the access engine is communicatively coupled to a repository comprising acceptable credentials, further wherein the access engine is operable to compare the unique identifier against the acceptable credentials as a part of granting access rights to the given user (Ueshima Fig. 1 item 60 and associated text, where it receives the data from a database).

8.15. As per claim 17, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 14, wherein the authentication request from the PPPoE client comprises an included identifier, further wherein the customizing engine is further operable to remove included identifier prior to an outputting of the authentication request to the access engine (As shown above, Ueshima teaches registering additional user information such as address, date of birth, etc. (see col. 13 lines 1-15) on the need of the service. Therefore, it would be obvious to submit such identifiers, as part of authentication request. Ueshima also teaches that in the second step of authentication, a password is submitted. Therefore, it would have been obvious to remove the identifiers used in the initial step of authentication, from the request in the second step of authentication. The motivation would be to prevent disclosure of plurality of user sensitive information, if the certificate is discovered by a malicious user. The certificate contains the parameters required for second step of authentication, and excludes the ones not necessary.

8.16. As per claim 18, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 14, wherein the authentication request from the PPPoE client comprises an included identifier that does not uniquely identify the given user (see response to claim 17, and note that, for example, the address does not identify the user uniquely).

8.17. As per claim 19, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 14, further comprising a piece of customer premises equipment comprising a broadband modem, the broadband modem operable to output the authentication request to the interface (as mentioned above, use of different types of network systems, which were well-known and broadly used at the time of invention, in combination of other networks would have been obvious to the one skilled in art. Examiner takes the Official Notice that broadband modems were well-known and widely used at the time of invention).

8.18. As per claim 20, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 19, further comprising a service provider network node that comprises the interface, the customizing engine, and the output device (item 30 of Fig. 1 of Ueshima includes all the required items, as discussed in claim 14).

8.19. As per claim 21, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 20, further comprising: a communication path operable to form at least a part of an interconnection between the broadband modem and the Public Internet (connection of a broadband modem to internet was well-known in the art, and therefore it would have been obvious to use the combination of Ueshima in view of Schneider, and further in view of Examiner Official Notice in conjunction with a network consisting a broadband modem connected to internet. Note that said connection makes a communication path); and the access engine, wherein the access engine is communicatively coupled to a repository comprising acceptable credentials, further wherein the access engine is operable to compare the unique identifier against the acceptable credentials as a part of granting the given user an access right to the communication path (These requirements were discussed in rejection of claims 1-20 above).

8.20. As per claim 22, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 21, wherein the unique identifier comprises a unique circuit identification number associated with an ADSL connection (see rejection of claim 6).

8.21. As per claim 23, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 21, wherein the unique identifier

comprises network generated information that is unique to a connection in use by the given user (the telephone number is unique).

8.22. As per claim 24, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the system of claim 23, wherein the unique identifier does not uniquely identify the piece of customer premises equipment or the broadband modem (the password is generated based on the phone number of the circuit id, and does not uniquely identify the piece of customer premises equipment).

8.23. The requirements of claim 25 are substantially the same as claims 1-14 as discussed in the Office Action dated 4/29/2008 and above. Note that sending a response to the user to notify them that the authentication had been successful, and the user is permitted to use the services was well-known and widely practiced at the time of invention. Therefore, sending the permit response upon acceptance of credentials would have been obvious to the one skilled in the art.

8.24. As per claim 26, Ueshima in view of Schneider, and further in view of Examiner Official Notice is directed to the computer-readable medium of claim 25, wherein the credential comprises a commonly assigned credential that does not uniquely identify a requestor (the password is generated based on the phone number of the circuit id, and does not uniquely identify the requestor).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

10/22/2008

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434